

System and method for providing protocol translation and filtering to access the world wide web from wireless or low-bandwidth networks

Patent number: JP11507152T

Publication date: 1999-06-22

Inventor:

Applicant:

Classification:

- international: **H04L29/06; H04L29/06;** (IPC1-7): G06F13/00;
G09C1/00; H04L12/54; H04L12/58

- european: H04L29/06; H04L29/06C6A; H04L29/06E; H04L29/06J1

Application number: JP19960533423D 19960326

Priority number(s): WO1996US03909 19960326; US19960614612
19960322

Also published as:

WO9735402 (A1)
EP0885501 (A1)
US5673322 (A1)
JP2003233541 (A)
CN1155197C (C)

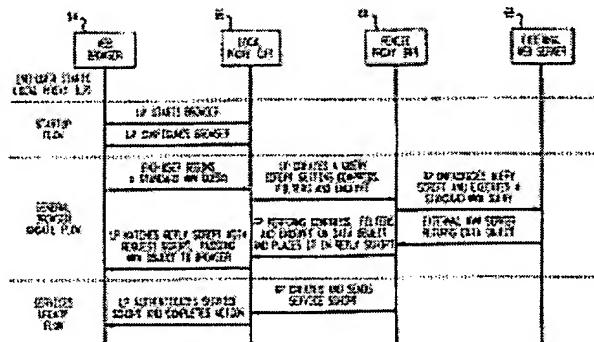
[more >>](#)

[Report a data error here](#)

Abstract not available for JP11507152T

Abstract of corresponding document: **US5673322**

An interface between a protected computer or computer network and the World Wide Web (WWW). The interface comprises a split proxy system that encapsulates TCP/IP transmissions into a script transmission, which is not subject to problems in high latency systems, thereby greatly improving WWW access, via a wireless modem or other low-bandwidth communications network. The split proxy interface also provides compression, encryption and filtering capabilities and allows receipt of unsolicited transmissions from the service provider for such purposes as automatically updating or configuring WWW access software.



Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表平11-507152

(43)公表日 平成11年(1999)6月22日

(51)Int.Cl.⁶
G 0 6 F 13/00
G 0 9 C 1/00
H 0 4 L 12/54
12/58

識別記号

F I
G 0 6 F 13/00
G 0 9 C 1/00
H 0 4 L 11/20

3 5 1 B
6 6 0 E
1 0 1 B

審査請求 有 予備審査請求 有 (全 49 頁)

(21)出願番号 特願平9-533423
(86) (22)出願日 平成8年(1996)3月26日
(85)翻訳文提出日 平成10年(1998)9月22日
(86)国際出願番号 PCT/US96/03909
(87)国際公開番号 WO97/35402
(87)国際公開日 平成9年(1997)9月25日
(31)優先権主張番号 08/614,612
(32)優先日 1996年3月22日
(33)優先権主張国 米国(US)
(81)指定国 EP(AT, BE, CH, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU,
MC, NL, PT, SE), AU, CA, CN, JP,
KR, MX, SG

(71)出願人 ベル コミュニケーションズ リサーチ,
インコーポレイテッド
アメリカ合衆国 07960 ニュージャージー
一州 モーリスタウン サウス ストリー
ト 445
(72)発明者 ベベ, ディヴィッド, マシュー
アメリカ合衆国 07748 ニュージャージー
一州 ミドルタウン キングス ハイウェ
イ 51
(74)代理人 弁理士 谷 義一 (外3名)

最終頁に続く

(54)【発明の名称】リモート・プロキシ・システムおよび方法

(57)【要約】

保護されているコンピュータまたはコンピュータ・ネットワーク(52)とワールド・ワイド・ウェブ(World Wide Web - WWW)(68)との間のインターフェースが開示されている。このインターフェースは分割プロキシ・システム(65、66)を含み、このシステムはTCP/IP伝送を高レイテンシ・システムで起こる問題に影響されないスクリプト伝送にカプセル化することによって、ワイヤレス・モdemまたは他の低バンド幅ネットワークからのWWWアクセスを大幅に向上している。この分割プロキシ・インターフェース(56、66)は圧縮、暗号化およびフィルタリングを行う能力も備え、WWWアクセス・ソフトウェアを自動的に更新または構成するといった目的のために、非送信請求伝送をサービス・プロバイダから受信することを可能にしている。

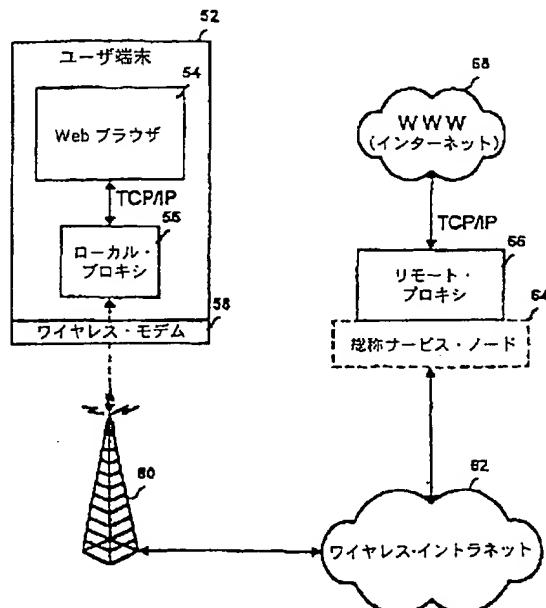


FIG. 2

【特許請求の範囲】

1. コンピュータ・ネットワークと通信する方法であつて、
　　ブラウザとローカル・プロキシをもつホスト・コンピュータを第1ロケーションに設置し、
　　低バンド幅ネットワークを通して前記ローカル・プロキシと通信するリモート・プロキシを第2ロケーションに設置し、
　　前記ブラウザで照会を開始し、アプリケーション層プロトコルを使用して前記照会を該ローカル・プロキシに送信し、
　　該照会の前記アプリケーション層プロトコルを前記低バンド幅ネットワーク上を伝送するのに適したトランスポート・プロトコルに変換し、
　　該照会を該低バンド幅ネットワークを利用して該ローカル・プロキシから前記リモート・プロキシに伝送し、
　　前記トランスポート・プロトコルを前記コンピュータ・ネットワークで該照会を実行するのに適したアプリケーション層プロトコルに変換することを含むことを特徴とする方法。
2. 請求項1に記載の方法において、前記照会をネットワーク・サーバに伝達し、該照会を実行し、データ・オブジェクトを前記リモート・プロキシに戻す前記ステップをさらに含むことを特徴とする方法。
3. 請求項2に記載の方法において、さらに、
　　前記データ・オブジェクトを前記低バンド幅ネットワーク上を伝送するのに適したトランスポート・プロトコルに変換し、
　　該データ・オブジェクトを該低バンド幅ネットワークを利用して前記リモート・プロキシから前記ローカル・プロキシに伝送し、
　　該データ・オブジェクトの前記トランスポート・プロトコルを該ローカル・プロキシでアプリケーション層プロトコルに変換し、
　　該データ・オブジェクトを前記アプリケーション層プロトコルを使用して前記ブラウザに伝達する前記ステップを含むことを特徴とする方法。
4. 請求項1に記載の方法において、スタートアップ・オペレーションをさらに含み、該スタートアップ・オペレーションは、

前記ホスト・コンピュータで前記ローカル・プロキシを始動し、
該ローカル・プロキシを使用して前記ブラウザを構成し、始動する前記ステップ
を含むことを特徴とする方法。

5. 請求項1に記載の方法において、前記照会の前記アプリケーション層プロ
トコルを変換する前記ステップは、さらに、

圧縮、フィルタ、および暗号化に関する設定値をもつ照会スクリプトを作成し

前記照会スクリプトをカプセル化して、前記低バンド幅ネットワークを利用して
前記ローカル・プロキシから前記リモート・プロキシに伝送する前記ステップ
を含むことを特徴とする方法。

6. 請求項5に記載の方法において、前記データ・オブジェクトの前記アリ
ケーション層プロトコルを変換する前記ステップは、さらに、

前記照会スクリプトに含まれる前記設定値に従って該データ・オブジェクトを
圧縮し、フィルタリングし、暗号化し、

該データ・オブジェクトを応答スクリプトに入れて、前記低バンド幅ネットワ
ークを利用して前記リモート・プロキシから前記ローカル・プロキシに伝送する
前記ステップを含むことを特徴とする方法。

7. 請求項6に記載の方法において、さらに、

前記応答スクリプトを前記ローカル・スクリプトで受信したとき該応答スクリ
プトを前記照会スクリプトと突き合わせ、

該応答スクリプトを前記ブラウザに送付し、

前記データ・オブジェクトを該応答スクリプトからアンパッケージし、

該データ・オブジェクトを該ブラウザのビュアで表示する前記ステップを含む
ことを特徴とする方法。

8. 請求項1に記載の方法において、さらに、

サービス・スクリプトを前記リモート・プロキシで作成し、

前記サービス・スクリプトを該リモート・プロキシから前記ローカル・プロキ
シに伝送し、

該サービス・スクリプトを解析し、要求アクションとデータ・オブジェクトを

該サービス・スクリプトから抜き出し、

サービス・アクションを該ローカル・プロキシで実行する前記ステップを含むことを特徴とする方法。

9. 請求項1に記載の方法において、前記コンピュータ・ネットワークは、World Wide Webであることを特徴とする方法。

10. コンピュータ・ネットワークと通信するシステムであって、

第1ロケーションに置かれていて、ブラウザとローカル・プロキシをもつホスト・コンピュータと、

第2ロケーションに置かれていて、低バンド幅ネットワークを通して前記ローカル・プロキシと通信するリモート・プロキシと、

前記ブラウザで照会を開始し、アプリケーション層プロコトルを使用して前記照会を該ローカル・プロキシに送信するリモート・プロキシと、

該照会の前記アプリケーション層プロトコルを前記低バンド幅ネットワーク上を伝送するのに適したトランスポート・プロトコルに変換する手段と、

該照会を該低バンド幅ネットワークを利用して該ローカル・プロキシから前記リモート・プロキシに伝送する手段と、

前記トランスポート・プロトコルを前記コンピュータ・ネットワーク上で該照会を実行するのに適したアプリケーション層プロトコルに変換する手段とを備えていることを特徴とするシステム。

11. 請求項10に記載のシステムにおいて、前記照会をネットワーク・サーバに伝達し、該照会を実行し、データ・オブジェクトを前記リモート・プロキシに戻す手段をさらに備えていることを特徴とするシステム。

12. 請求項11に記載のシステムにおいて、さらに、

前記データ・オブジェクトを前記低バンド幅ネットワーク上を伝送するのに適したトランスポート・プロトコルに変換する手段と、

該データ・オブジェクトを該低バンド幅ネットワークを利用して前記リモート・プロキシから前記ローカル・プロキシに伝送する手段と、

該データ・オブジェクトのトランスポート・プロトコルを該ローカル・プロキ

シでアプリケーション層プロトコルに変換する手段と、
前記アプリケーション層プロトコルを使用して該データ・オブジェクトを前記

ブラウザに伝達する手段とを備えていることを特徴とするシステム。

13. 請求項10に記載のシステムにおいて、さらに、
前記ローカル・プロキシを前記ホスト・コンピュータで始動する手段と、
該ローカル・プロキシを使用して前記ブラウザを構成し、始動する手段とを備
えていることを特徴とするシステム。

14. 請求項10に記載のシステムにおいて、前記照会の前記アプリケーション
層プロトコルを変換する前記手段は、さらに、
圧縮、フィルタ、および暗号化に関する設定値をもつ照会スクリプトを作成す
る手段と、

前記照会スクリプトをカプセル化し、前記低バンド幅ネットワークを利用して
前記ローカル・プロキシから前記リモート・プロキシに伝送する手段とを含んで
いることを特徴とするシステム。

15. 請求項14に記載のシステムにおいて、前記データ・オブジェクトの前記
アプリケーション層プロトコルを変換する前記手段は、さらに、
前記照会スクリプトに含まれる設定値に従って前記データ・オブジェクトを圧
縮し、フィルタリングし、暗号化する手段と、

該データ・オブジェクトを応答スクリプトに入れて、前記低バンド幅ネットワ
ークを利用して前記リモート・プロキシから前記ローカル・プロキシに伝送する
手段とを含んでいることを特徴とするシステム。

16. 請求項15に記載のシステムにおいて、さらに、
前記応答スクリプトを前記ローカル・プロキシで受信したとき該応答スクリプ
トを前記照会スクリプトと突き合わせる手段と、
該応答スクリプトを前記ブラウザに送付する手段と、
該データ・オブジェクトを該応答スクリプトからアンパッケージする手段と、
該データ・オブジェクトを該ブラウザのビュアで表示する手段とを備えている
ことを特徴とするシステム。

17. 請求項10に記載のシステムにおいて、さらに、
サービス・スクリプトを前記リモート・プロキシで作成する手段と、
前記サービス・スクリプトを該リモート・プロキシから前記ローカル・プロキ
シに伝送する手段と、
該サービス・スクリプトを解析し、要求アクションとデータ・オブジェクトを
該サービス・スクリプトから抜き出す手段と、
サービス・アクションを該ローカル・プロキシで実行する手段とを備えている
ことを特徴とするシステム。
18. 請求項10に記載のシステムにおいて、前記低バンド幅ネットワークはワ
イヤレス・ネットワークを含むことを特徴とするシステム。
19. 請求項10に記載のシステムにおいて、前記コンピュータ・ネットワーク
はWorld Wide Webを含むことを特徴とするシステム。
20. コンピュータ・ネットワークと通信するシステムであって、
ユーザ・インターフェースのためのブラウザをもつホスト・コンピュータと、
アプリケーション層プロトコルを使用して前記ブラウザと通信するローカル・
プロキシ手段であって、該ローカル・プロキシ手段は前記アプリケーション層プ
ロコトルをトランスポート・プロトコルに変換する手段をもつものと、
前記トランスポート・プロトコルを使用して該ローカル・プロキシ手段と通信
するリモート・プロキシ手段であって、該リモート・プロキシ手段は前記トラン
スポート・プロトコルを該アプリケーション層プロトコルに変換する手段をもち
、該リモート・プロキシ手段は該アプリケーション層プロトコルを使用して前記
コンピュータ・ネットワークと通信する手段をもつものとを備えていることを特
徴とするシステム。
21. 請求項20に記載のシステムにおいて、前記ローカル・プロキシと前記リ
モート・プロキシは低バンド幅ネットワークを通して通信することを特徴とする
システム。
22. 請求項20に記載のシステムにおいて、前記ローカル・プロキシと前記リ
モート・プロキシはワイヤレス・ネットワークを通して通信することを特徴とす

るシステム。

23. セキュアド・コンピュータ・ネットワーク・インターフェースであつて、

保護コンピュータまたはコンピュータ・ネットワークと、

公衆コンピュータ・ネットワークと、

前記保護コンピュータまたはコンピュータ・ネットワークと通信ネットワークとを接続するローカル・プロキシと、

前記通信ネットワークと前記公衆コンピュータ・ネットワークとを接続するリモート・プロキシとを備え、

前記プロキシはデータ伝送を暗号化する少なくとも1つの暗号化アルゴリズムを備えていることを特徴とするセキュアド・コンピュータ・ネットワーク・インターフェース。

24. 請求項23に記載のセキュアド・コンピュータ・ネットワーク・インターフェースにおいて、前記コンピュータ・ネットワークと前記公衆コンピュータ・ネットワークとの間のコネクションを所有または維持管理するサービス・プロバイダをさらに含み、前記少なくとも1つの暗号化アルゴリズムは前記サービス・プロバイダが前記保護コンピュータまたはコンピュータ・ネットワークにアクセスできるように該サービス・プロバイダに知られていることを特徴とするセキュアド・コンピュータ・ネットワーク・インターフェース。

25. 請求項24に記載のセキュアド・コンピュータ・ネットワーク・インターフェースにおいて、前記サービス・プロバイダは前記保護コンピュータまたはコンピュータ・ネットワーク上のソフトウェアを更新または構成する目的で保護コンピュータまたはコンピュータ・ネットワークにアクセスすることを特徴とするセキュアド・コンピュータ・ネットワーク・インターフェース。

26. コンピュータ・ネットワーク・インターフェースを安全保護する方法であつて、

保護すべきコンピュータまたはコンピュータ・ネットワークを準備し、

前記保護コンピュータまたはコンピュータ・ネットワークと通信ネットワークをローカル・プロキシと接続し、

前記通信ネットワークと公衆コンピュータ・ネットワークをリモート・プロキシと接続し、

前記ローカル・プロキシと前記ローカル・プロキシにデータ伝送を暗号化する少なくとも1つの暗号化アルゴリズムを装備させるステップを含むことを特徴とするコンピュータ・ネットワーク・インターフェースを安全保護する方法。

27. 請求項26に記載のコンピュータ・ネットワーク・インターフェースを安全保護する方法において、さらに、

前記通信ネットワークと前記公衆コンピュータ・ネットワークとの間のコネクションを管理し、

該通信ネットワークと該公衆コンピュータ・ネットワークとの間の前記コネクションを管理するサービス・プロバイダに少なくとも1つの暗号化アルゴリズムを提供するステップを含むことを特徴とする方法。

28. 請求項27に記載のセキュアド・コンピュータ・ネットワーク・インターフェースにおいて、前記少なくとも1つの暗号化アルゴリズムを使用して前記保護コンピュータまたはコンピュータ・ネットワークにアクセスして、前記サービス・プロバイダが該保護コンピュータまたはコンピュータ・ネットワーク上のソフトウェアを更新または構成できるようにするステップをさらに含むことを特徴とするセキュアド・コンピュータ・ネットワーク・インターフェース。

29. フィルタリング・コンピュータ・ネットワーク・インターフェースであって

保護コンピュータまたはコンピュータ・ネットワークと、

公衆コンピュータ・ネットワークと、

前記保護コンピュータまたはコンピュータ・ネットワークと通信ネットワークとを接続するローカル・プロキシと、

前記通信ネットワークと前記公衆コンピュータ・ネットワークとを接続するリモート・プロキシとを備え、

前記リモート・プロキシは該公衆コンピュータ・ネットワークから該保護コンピュータまたはコンピュータ・ネットワークへのデータ伝送をフィルタリングす

ることを特徴とするフィルタリング・コンピュータ・ネットワーク・インターフェース。

30. コンピュータ・ネットワーク・インターフェースを通してデータをフィルタリングする方法であつて、

保護コンピュータまたはコンピュータ・ネットワークを準備し、

前記保護コンピュータまたはコンピュータ・ネットワークと通信ネットワーク

をローカル・プロキシと接続し、

前記通信ネットワークと公衆コンピュータ・ネットワークをリモート・プロキシと接続し、

前記公衆コンピュータ・ネットワークから該保護コンピュータまたはコンピュータ・ネットワークへのデータ伝送を前記リモート・プロキシでフィルタリングするステップを含むことを特徴とする方法。

31. データを圧縮するコンピュータ・ネットワーク・インターフェースであつて

加入者コンピュータまたはコンピュータ・ネットワークと、

公衆コンピュータ・ネットワークと、

前記加入者コンピュータまたはコンピュータ・ネットワークと通信ネットワークとを接続するローカル・プロキシと、

前記通信ネットワークと前記公衆コンピュータ・ネットワークとを接続するリモート・プロキシとを備え、

前記プロキシは該公衆コンピュータ・ネットワークと該加入者コンピュータまたはコンピュータ・ネットワークとの間のデータ伝送を圧縮することを特徴とするデータを圧縮するコンピュータ・ネットワーク・インターフェース。

32. コンピュータ・ネットワーク・インターフェースを使用してデータを圧縮する方法であつて、

加入者コンピュータまたはコンピュータ・ネットワークを準備し、

前記加入者コンピュータまたはコンピュータ・ネットワークと通信ネットワークをローカル・プロキシと接続し、

前記通信ネットワークと公衆コンピュータ・ネットワークをリモート・プロキシと接続し、

前記公衆コンピュータ・ネットワークと該加入者コンピュータまたはコンピュータ・ネットワークとの間のデータ伝送を前記ローカル・プロキシと前記リモート・プロキシで圧縮するステップを含むことを特徴とするコンピュータ・ネットワーク・インターフェースを使用してデータを圧縮する方法。

付録A

頭字語一覧

CDPD セルラ・ディジタル・パケット・データ (Cellular Digital Packet Data)

FTP ファイル転送プロトコル (File Transfer Protocol)

HTML ハイパーテキスト・マークアップ言語 (Hyper Text Markup Language)

HTTP ハイパーテキスト・トランスポート・プロトコル (Hyper Text Transport Protocol)

IP インターネット・プロトコル (Internet Protocol)

ISDN 統合サービス・ディジタル網 (Integrated Services Digital Network)

ISG 統合サービス・ゲートウェイ (Integrated Services Gateway)

ISP インターネット・サービス・プロバイダ (Internet Service Provider)

LAN ローカル・エリア・ネットワーク (Local Area Network)

LP ローカル・プロキシ (Local Proxy)

LZW Lev-Zempel-Welch

OSI 開放型システム間相互接続 (Open Systems Interconnection)

PCI パーソナル・コミュニケーションズ・インターネット (Personal Communications Internetwork)

PDA パーソナル・ディジタル・アシスタント (Personal Digital Assistant)

stant)

R P リモート・プロキシ (Remote Proxy)

S M T P シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)

S S L セキュア・ソケット層 (Secure Socket Layer)

T C P 伝送制御プロトコル (Transmission Control Protocol)

U D P ユーザ・データグラム・プロトコル (User Datagram Protocol)

U R L 汎用リソース・ロケータ (Universal Resource Locator)

W A I S 広域情報検索 (Wide Area Information Search)

W W W ワールド・ワイド・ウェブ (World Wide Web)

【発明の詳細な説明】

リモート・プロキシ・システムおよび方法

発明の背景

関連特許出願

米国特許出願第08/309,336号（1994年9月19日出願、発明者：David Mathew Pepe、Lisa B. Blitzer、James Joseph Brockman、William Cruz、Dwight Omar Hakim、Michael Kramar、Dawn Dian Petr、Josefa Ramaroson、Gerardo Ramirez、Yang-Wei Wang、およびRobert G. White）は本件出願に関連する主題を開示しており、この米国出願を引用することにより、本明細書の一部を構成するものである。

発明の分野

本発明は、私用コンピュータまたは私用コンピュータ・ネットワークと、ワイアライン（有線）接続とワイヤレス（無線）接続の両方を使用するワールド・ワイド・ウェブ（World Wide Web-WWW）との間の改良インターフェースに関する。特に、本発明は、プロトコル変換、セキュリティおよび自動構成の特徴を備えた改良WWWインターフェースに関する。

関連技術の説明

この50年の間、人々が夢見ていたことは汎用情報データベースである。すなわち、世界中の人達がアクセス可能であるだけでなく、関連情報が容易に見つかるように、さらに、特定の要求を満たす最も関連のあるデータがユーザによって即時に見つけられて、アクセスされるように編成されたデータである。

1960年代には、この考え方はさらに検討され、「ドキュバース（docuverse）」というビジョンが生まれ、あらゆる側面から見た人間と情報とのやりとりに、特に教育分野において大変革がもたらされるになった。これらのビジョンを現実化し、地球規模でこのビジョンを実現化することを可能にするテクノロジが現れたのはつい最近のことである。

インターネット（The Internet）は大学、企業および政府の共同作業によって発

達してきた。数年前に、米国国防総省は共同で研究を実施していた大学と私的団体および、時には、企業のコンピュータ・ネットワークを相互接続することを開始した。このネットワークのネットワークは、やがては、一般にインターネットまたはワールド・ワイド・ウェブ(World Wide Web-WWW)と呼ばれているグローバル・ネットワークに発達するに至った。WWWの正式の説明は、「大規模のドキュメントへの汎用アクセスを可能にすることを目的とした広域ハイパーテディア情報検索イニシアティブ」となっている。

WWWが普及して、一般に広く使用されるようになると、米国国防総省はWWWへの関与を縮小していった。今日では、インターネット上の多くの政府資金に基づくリンクは、大学、会社などの間のローカル・エリア・ネットワ(Local Area Network-LAN)の相互接続を運営している商業目的の企業に移譲されている。

WWWは企業にとって極めて貴重な資源であること(電子メール(eメール)による通信、オンラインによる情報アクセスなどの目的のために)が実証されつつあるが、企業が関心を持っているのは、コンピュータ・ネットワーク上にストアされている自社の知的財産権、トレードシークレット、財務記録および他の機密情報のセキュリティ(安全保護)である。また、電子破壊(コンピュータ化情報を破壊または歪曲する目的でWWW上でコンピュータ・ネットワークに無許可でアクセスすること)にも関心を持っている。

これらの関心事に応えるために、WWWへのある種の接続(コネクション)は「ネットワーク・セキュリティ・ファイアウォール(Network Security Firewall)」で保護されている。図1に示すように、ファイアウォールとは、私用コンピュータまたはコンピュータ・ネットワーク(LAN)10とWWW 12との間の接続をブリッジする特定のハードウェア部分および/またはソフトウェア部分のことである。ファイアウォールの主目的は、保護すべきネットワークに入出力されるデータ・トラフィックをスクリーニングすることである。ネットワーク侵入者が検出されたとき、ファイアウォールはデータ・トラフィックにふるいをかけて、侵入者のアクセスを不能にする機能をもっている。初期形態のインターネット・ファイアウォールでは、どのデータ・トラフィックが正しいか、正しくな

いか、つまり、企業ユーザに関係するものか侵入者に関係するものかを確かめることが

一般的に困難であった。このことは、ファイル転送プロトコル(File Transfer Protocol-F T P)などのインターネット・アプリケーションの企業ユーザ(企業内L A N内の)にとっては、そのアプリケーションがファイアウォールによって誤ってブロックされることがあるために問題となっていた。望ましいトラフィックが妨げられないようにするためには、ファイアウォールは、ファイアウォールを通り抜けるアプリケーション・データに関するより多くの情報を必要としていた。

インターネットのエンジニアは、この要求に応えるためにインターネット・ファイアウォール上に「プロキシ(proxy)」サービスを設計した。これらのプロキシは、F T Pアプリケーションのような特定アプリケーションを完全に理解するコンピュータ・プロセスである。企業内ユーザが実行したいと思っているアプリケーションのタイプに基づいて複数のプロキシをファイアウォール・システムに追加することは、ネットワーク管理者にとっては容易な問題となった。例えば、WWWブラウザ(後に述べる)はハイパーテキスト・トранSPORT・プロトコル(Hyper Text Transport Protocol-H T T P)プロキシを使用してハイパーテキスト・マークアップ言語(Hyper Text Markup Language-H T M L)ドキュメントを転送している。

WWWの使用を容易にするために、「ブラウジング」ソフトウェア6が開発された。よく知られたNetscape(商標)ブラウザやMosaic(商標)ブラウザのようなブラウザを使用すると、WWWユーザはWWWにリンクされたコンピュータ上で利用可能な情報をブラウズすることができる。米国特許出願第08/309, 336号(以下、' 3 3 6出願という)に記載されている、本件出願の被譲渡人による関連発明では、コンピュータ・ネットワーク上のユーザが、統一化された手段を使用して種々のメディアに単純な方法でアクセスすることを可能にしている。³ ' 3 3 6出願の発明では、ブラウジング・ソフトウェアを利用することにより、人々による情報の表示方法と作成方法を変更した。つまり、この発明は最初の真のグ

ローバル・ハイパー・メディア・ネットワークを構築した。

H T T P プロキシが受け持つ1つの役割は、保護ネットワーク10内のブラウザまたはソフトウェア・アプリケーションからの要求を受信し、その要求をWWW 12に中継することである。このプロキシはWWW 12からの保護コンピ

ュータまたはネットワーク10へのアクセスもモニタしている。従って、プロキシ4を使用すると、システム管理者は保護ネットワーク10とWWW 12の間を流れる情報と要求をモニタすることができる。違法なアクティビティが見つかると、プロキシ4はWWW 12との接続を中断することができる。このプロキシ駆動型ファイアウォール(proxy-driven firewall) 2, 4を使用すると、企業および類似の関心事をもつ企業はある程度のセキュリティを保ちながら、WWW 12の貴重資源を利用することができる。

コンピュータとソフトウェア・アプリケーションとを結ぶリンクをWWW上で実現するために、コンピュータ化データの伝送を規律するプロトコルがいくつか開発されている。あるプロトコルはWWW上を伝送されるデータを、受信側コンピュータが認識できる標準的方法で編成している。コンピュータ・プロトコルの開放型システム間相互接続(OSI)モデルは7つの層からなっている。各層は付加的な編成上の機能を追加していき、データの伝送を容易化している。

インターネット・プロトコル(Internet Protocol-IP)はOSIモデルの第3層であり、インターネット上で話される基本的「言語」となっている。第4層である伝送制御プロトコル(Transmission Control Protocol-TCP)はIPに含まれる、より特殊化されたプロトコルである。WWWを使用するには、コンピュータはIP、従って、TCPを組み込んでいるプロトコルを使用して通信できなければならない。

インターネット・アクセスを取り巻くWWWとテクノロジは爆発的な成長を遂げている。多くの企業は、加入者が標準テレホニを使用してWWWにアクセスすることを可能にするまでに発達している。インターネット・サービス・プロバイダ(Internet Service Provider-ISP)と呼ばれるグループは、これらのサービス・プロバイダの多くを代表している。

インターネット・アクセスのさらなる拡張が見込まれる分野として、広域ワイヤレス・データ・ネットワークがある。ワイヤレス・ネットワークには、セルラ・ディジタル・パケット・データ(cellular digital packet data-CDPD)。セルラキャリヤから提供されている) ネットワーク、Mobitex(商標) ネットワーク(米国内のRAM Mobile dataによって提供されている)などの回線交換セルラ・ネ

ットワーク、Ardis(商標)ネットワーク、および各国で台頭している多数のワイヤレス・データ・プロバイダがある。

上述したデータ・ネットワーク・プロバイダはすべて従来のインターネット・プロトコル(IP)サービスを提供し、WWWと統合化できる能力を備えている。データ速度は4,800 bpsから28,800bpsの範囲であり、そのレイテンシはミリ秒単位から10秒の範囲である。

WWWの人気にもかかわらず、インターネットにアクセスするとき解決しなければならない技術上の問題と、セキュリティ上の問題が残っている。これらの問題のいくつかは、WWWにアクセスしようとするワイヤレス・システムの場合には特に深刻である。

問題1

最初の問題はデータ・レイテンシが原因で起こる問題である(詳細は後述する)。データ・レイテンシとは、データがWWW内の種々のノードを通過するとき複数のホップ(hop)と低速リンクで引き起こされる時間遅延のことである。この特殊な問題はWWWがワイヤレス・モジュムを使用してアクセスされるときは、さらに悪化している。大部分の広域ワイヤレス・データ・ネットワークと一部のワイヤライン・データ・ネットワークは、元来TCP/IPプロトコルをサポートする設計になっていない。レイテンシはIPデータをネットワークのオリジナル・データ・プロトコルにカプセル化するとさらに増加する。

TCPはWWW上で伝送するデータを編成するとき、そのデータを離散的情報「パケット」に分割する。その後、TCPは個々のパケットを送信する。各パケットは受信側システムに対する指示を含み、パケットはこの指示に従って完全

データ構造に再組み立てされて、送信される。また、各パケットは巡回冗長チェックも含んでおり、パケットが伝送中に壊されなかつたか、あるいは分断されなかつたかを受信側システムがチェックできるようになっている。

TCPは、複数のパケットを送信したあと、そのパケットが正しく受信されたとの受信側システムからの確認通知を待つように構成されているのが一般的である。データ・パケットを送信してから、その到着確認通知を受信するまでに要する時間量はシステムの「レイテンシ」として知られている。

TCPはデータ・パケットが正しく受信されたとの確認通知を受信しないときは、パケットが送信中に失われたものとみなして、パケットを再送信する。システムのレイテンシが余りに高くなると、TCPはパケットが失われたものと早合点するため、オリジナル・パケットがそのデスティネーション（宛て先）に到着する前にネットワークは同じデータ・パケットの再送であふれることになる。多くのサービス・プロバイダは送信されるデータ・パケットごとにユーザに料金請求しているので、これも1つの問題となっている。TCPが、まだ送信中のパケットと重複する不要なパケットでシステムをあふれさせると、ユーザの費用負担は大幅に増加することになる。従って、TCPは高レイテンシの接続では正しく動作できることになる。システムのレイテンシがほぼ3秒から5秒の範囲を越えると、TCPは誤動作を始めることになる。

WWWがTCPをサポートしていない標準電話回線でアクセスされるときは、TCPデータグラムは電話回線で送信できる形式にカプセル化（つまり、変換）されなければならない。このデータグラムは受信側コンピュータでアンパックされてから使用される。この手法は効果的であるが、伝送のレイテンシが増加することになる。

ワイヤレス・モ뎀を使用してWWWにアクセスするとき起こる、もう1つの問題はワイヤレス・ネットワークによって引き起こされるレイテンシの増加である。ワイヤレス・データ・ネットワークがサービスするエリアが広くになると、伝送のバンド幅（bps 単位）が低下するのが一般的傾向である。例えば、米国で使われている現存ワイヤレス通信システムは毎秒4,800ビットのデータを送信す

る能力をもっている。この結果、レイテンシは10秒までに達している。

ワイヤレスWWWアクセスに関する現存の関連技術として次のものがある。

1. Carnegie Mellon University の Information Networking Institute, Wireless Andrew Initiative,
2. Rutgers University の Winlab, Dataman project,
3. University of Washington の CS & E, Mobisaidc,
4. Xerox社の Palo Alto Research Center, RDA および virtual office computing concepts
5. Computer Networks & ISDN Systems Volume 0028, Number 1-2 ISSN:0169-7552, Dec'98, "PDAs as Mobile WWW Browsers", Gessler S., Kotulla A..
6. General

Magic社の Magicap OS version of a WWW browser with enhancements for Telescript agent technology (Telescriptエージェント・テクノロジ用の強化機能を備えた Magicap OS バージョンの WWW ブラウザ)。

上記のプロジェクトおよび論文のすべては、ブラウザの修正、新しいプロトコルの規格（この場合も TCP をベースとする）、またはワイヤレスおよび低バンド幅のネットワークをインターネットに接続して WWW アクセスを可能にする一般的なインターネット接続規格の定義を必要としている。

従って、高レイテンシのワイヤレスおよびワイヤライン・ネットワーク上のコミュニケーションにおいて、TCP を変換する方法が要望されている。

問題2

第2の問題は、現存の WWW アクセス・ソフトウェアには、圧縮、暗号化、またはフィルタリングのための標準的メカニズムが備わっていないことである。圧縮を行うと、情報の内容を変更することなくデータ・サイズが縮小されてネットワーク上を伝送される。圧縮をサポートする大部分のプロトコルは ブラウザからの外部ユーティリティを必要とし、データを伸張したあとで、多目的インターネット・メール・エクステンション (Multipurpose Internet Mail Extension-MIME, Nathaniel Borenstein et.al RFC1521) タイプの使用を通して有用な出力を ブラウザに戻すようにしている。

暗号化は、データ伝送を符号化したものである。暗号化を行うと、暗号化され

たデータ伝送を無許可の当事者が理解し、アクセスすることがはるかに困難になるのでセキュリティ（機密保護）が得られる。残念ながら、これらの望ましいサービスの一般的で、開放型の標準を、すべてのWWWクライアント要求をサポートするように作成できるという見通しがない。WWWソフトウェア（つまり、セキュア・ソケット層(Secure Socket Layer-S S L)）での暗号化に関する標準は発展途上にある。しかし、現在のコンピュータ・ハッキングのレベルでは、暗号化に関するどの開放型標準も、インテグリティ（保全性）を長時間保持できるという見通しがない。

従って、大部分のアドバンスド・ブラウジング・テクノロジは自社所有暗号化方式をインストールしているため、その暗号化方式をサポートするWWWサーバ

の間でしか働くことができない。このオプションはWWWの開放型標準設計に逆行するものである。

フィルタリングとは、WWW応答をデータのサイズ、タイプまたは他の特性に基づいてグローバルで制御することであり、これによってユーザはデータの受信をカスタマイズすることができる。作業は、WWWサーチ・エンジン、アドバンスド・ブラウザ上の特殊化されたキャッシング・ユーティリティなどを通してこのエリアで行われている。

ここで言うフィルタリングは、余りに多いデータを要求するか、擬似情報を検索することにより、あるいはWWW要求が原因で起こるその他の望ましくない副作用によって、ワイヤレス／低バンド幅データ・ネットワークを誤用するおそれのある、不注意なユーザのためのグローバル・セーフティ・ネットである。例えば、ユーザは、送信するには極めて大きく、おそらくコストがかかるとユーザが気づいていないデータ・オブジェクトをWWWに要求することがある。セーフティ・ネットでは、ユーザは特定の要求が実行されるのを自動的に防止するようフィルタを構成することができる。

従って、圧縮、暗号化およびフィルタリングの機能をWWWインターフェースに実装することが要望されている。

問題 3

第3の問題は、WWWアクセス・ソフトウェアが非同期または非送信請求(unolicited)更新をネットワークから受信するための標準的方法がないことである。Netscape(商標)、Mosaic(商標)、Lynx(商標)ブラウザなどの最も人気のあるブラウザは人気度の劣る他のブラウザと同様に、応答データがそれぞれのブラウザに送られる前にユーザがなんらかの形態の応答を出すことを要求している。

例えば、望ましいことは、WWWへのアクセス権を持つ企業が、加入者のWWWアクセス・システムをネットワーク内からリモートで構成できるようにすることである。正規のブラウザはこの機能を備えていないので、加入者は各自のアクセス・ソフトウェアを手作業で構成し、更新しなければならない。これを行うには、従来の音声カストマ・サポート・ラインまたはユーザのホスト・システム上のカスタム・エージェント・ソフトウェアを通して、サービス・プロバイダのサポートが必要になる(この問題の詳しい説明は、「ISG:統合化サービス・ゲートウェイ(ISG: Integrated Services Gateway)」、Bellcore TM-2485 6に記載されている)。

従って、特に、ネットワークをアクセスするためのソフトウェアの構成を自動化するために、ネットワークまたはサービス・プロバイダからの非送信請求伝送を受信し、実現できるWWWインターフェースが要望されている。

発明の概要

以上に鑑みて、本発明の目的は、上述した要求およびその他のことに応えることである。本発明の目的は、WWWとのインターフェースとなって、高レイテンシ環境でTCP/IPをサポートし、圧縮、暗号化およびフィルタリング・サービスを提供し、WWWまたはサービス・プロバイダからの非送信請求メッセージ(unolicited message)を受け取って、実現する方法およびシステムを提供することである。

本発明のその他の目的、利点および新規の特徴は後述する説明に記載されているが、これらはその説明を読み、本発明を実施することによりこの分野の当業者に容易に理解されるはずである。本発明の目的と利点は、請求の範囲に記載され

ている事項によって実現し、達成することが可能である。

上述した目的およびその他の目的を達成するために、また以下で具現化され、広義に説明されている本発明の目的によれば、本発明のシステムと方法は、第1ロケーションに置かれていて、ブラウザとローカル・プロキシをもつホスト・コンピュータ、第2ロケーションに置かれていて、低バンド幅ネットワークを通してローカル・プロキシと通信するリモート・プロキシ、ブラウザ上で照会(query)を出し(initiate)、アプリケーション層プロトコルを使用してその照会をローカル・プロキシに送信する手段、照会のアプリケーション層プロトコルを低バンド幅ネットワーク上で送信するのに適したトランスポート・プロトコルに変換する手段、照会を低バンド幅ネットワークを通してローカル・プロキシからリモート・プロシキに送信する手段、および、トランスポート・プロトコルをコンピュータ・ネットワーク上で照会を実行するのに適したアプリケーション層プロトコルに変

換する手段、を利用している。

また、好ましくは、本発明のシステムと方法は、照会をネットワーク・サーバに伝達し、その照会を実行し、データ・オブジェクトをリモート・プロキシに返送する手段、そのデータ・オブジェクトを低バンド幅ネットワーク上で送信するのに適したトランスポート・プロトコルに変換する手段、データ・オブジェクトを低バンド幅ネットワークを通してリモート・プロキシからローカル・プロシキに送信する手段、データ・オブジェクトのトランスポート・プロトコルをローカル・プロキシでアプリケーション層プロトコルに変換する手段、および、アプリケーション層プロトコルを使用してデータ・オブジェクトをブラウザに伝送する手段を含んでいる。

また、好ましくは、本発明のシステムと方法は圧縮、フィルタリングおよび暗号化の設定をもつ照会スクリプトを作成する手段、照会スクリプトをカプセル化(encapsulating)して低バンド幅ネットワークを通してローカル・プロキシからリモート・プロキシに送信する手段、照会スクリプトにおける設定に従ってデータ・オブジェクトを圧縮し、フィルタリングし、暗号化する手段、および、データ

タ・オブジェクトを応答スクリプトに入れて低バンド幅ネットワークを通してリモート・プロキシからローカル・プロキシに送信する手段を含んでいる。

本発明の他の形態では、その目的と用途によれば、本発明のシステムは、コンピュータ・ネットワークと通信するシステムを含むことも可能であり、このシステムは、ユーザ・インターフェースのためのブラウザをもつホスト・コンピュータ、アプリケーション層プロトコルを使用してブラウザと通信するローカル・プロキシ手段(このローカル・プロキシ手段はアプリケーション層プロコトルをトランスポート・プロトコルに変換する手段を含んでいる)、および、トランスポート・プロトコルを使用してローカル・プロキシ手段と通信するリモート・プロキシ手段を含んでいる。リモート・プロキシ手段は、トランスポート・プロトコルをアプリケーション層プロトコルに変換する手段、および、アプリケーション層プロトコルを使用してコンピュータ・ネットワークと通信する手段を含んでいる。

図面の簡単な説明

以下では、本発明の理解を容易にするために添付図面を参照して本発明の内容

を開示しながら説明する。添付図面において、

図1は、私用コンピュータ・ネットワークとWWWとの間の、従来技術による、ファイアウォール・インターフェースを示すブロック図である。

図2は、本発明の分割プロキシ・インターフェースを示すブロック図である。

図3は、本発明のローカル・プロキシ・インターフェースによって実行されるプロトコル変換を示す説明図である。

図4は、本発明のリモート・プロキシ・インターフェースによって実行されるプロトコル変換を示す説明図である。

図5は、本発明のプロキシ・インターフェースにおける実施(インプリメンテーション)を示すフローチャートである。

好適実施例の詳細な説明

以下、添付図面に図示している例を参照して、本発明の好適実施例について詳しく説明する。

WWWの構築はコンピュータ革命であり、これはワイヤレス・データ・ネットワークが爆発的なインターネットの人気に直接に参加できるようにする潜在的触媒ともなっている。本発明は、私用コンピュータまたは私用コンピュータ・ネットワークをWWWと結ぶインターフェースとなって、高レイテンシ環境でTCP/IPをサポートし、圧縮、暗号化およびフィルタリング・サービスをサポートし、サービス・プロバイダによって送信される非送信請求メッセージの受信と実現をサポートする方法およびシステムを提供する。また、本発明によれば、ラップトップ(Laptop)またはパーソナル・ディジタル・アシスタント(Personal Digital Assistant-PDA)が移動通信(ワイヤレス)端末からWWWに直接アクセスすることを可能にしている。

例えば、本発明によるWWWとのインターフェースは、必要とする機能を実行するようにプロキシ(図1のエレメント4)を改良することにより実現することが可能である。この改良型プロキシは分割プロキシのシステム(米国特許出願第08/309,336号に記載されているように、エージェント・テクノロジと呼ばれることもある)になり、これはファイアウォール上に実現することも、あるいはワイヤレスまたはワイヤライン・ネットワークからWWWにアクセスできる個人コンピュータ(ラップトップでもよい)上でバックグラウンドで実行されるアプリケーションにすることもできる。

図2に示すように、本発明のインターフェースは改良型分割プロキシ(modified split proxy)である。分割プロキシはローカル・プロキシ56とリモート・プロキシ66を含み、これらのプロキシはWWW要求の変換(translation)と復元(restoration)を可能にするソフトウェア・モジュールである。

モバイル端末52を操作するユーザはTCP/IPを使用してWWWと通信するWebブラウザ54を使用している。ローカル・プロキシ56は、ユーザ端末52上でバックグラウンドで実行されるソフトウェア・パッケージである。高レイテンシが問題になっている場合は、ローカル・プロキシ56は、本発明の原理によれば、ブラウザによって使用されるTCP/IPプロトコルと、通信ネットワーク上をリモート・プロキシまでデータを運ぶのに十分強固なプロトコルとの間

でデータ要求／伝送を変換する。

図2に示す実施例では、ユーザはワイヤレス・ネットワークを通してWWWにアクセスしている。例えば、ワイヤレス・モデム58はAirBoss(商標)ワイヤレス・トランスポート・プロトコルなどの、低バンド幅最適化プロトコル(*low-bandwidth optimized protocol*)を使用して、ベースステーション(基地局)60と通信している。従って、ローカル・プロキシ56は低バンド幅最適化プロトコルをTCP/IPに変換する。

ローカル・プロキシのカプセル化要求スクリプト(図5の一般ブラウザ使用フローを参照)はワイヤレス・ネットワーク62を通してリモート・プロキシ66に送信される。リモート・プロキシ66はTCP/IPと、AirBoss(商標)トランスポート・プロトコルなどの低バンド幅最適化プロトコルとの間で必要なプロコトル変換を行って、ユーザをWWW 68に接続する。

本発明には、プロキシ・サービスをサポートする標準Webブラウザを、ワイヤレスおよび低バンド幅のWebブラウジングに適応できるようにするメソッドがいくつか用意されている。以下の本発明の説明では、上述した第1、第2、および第3の問題にそれぞれ関係する3セットのメソッドについて説明する。

メソッド・セット1

解消すべき第1の問題は例えば、約3秒から5秒を越える高レイテンシを引き起こすネットワーク上をTCP/IPを使用してデータを伝送する場合である。問題1を解決するために使用される方法とシステムでは、プロトコル変換が行われる。プロトコル変換とは、要求と応答が1つのペアになっているTCPアプリケーション要求(つまり、HTTP、SMTP、Gopher、およびWAIS)を、データを伝送する通信ネットワーク、特にワイヤレス・ネットワークやその他の低バンド幅ネットワーク上で起こる高レイテンシでも機能できるだけの強固な、適切なコネクション型プロトコル(*connection-oriented protocol*)にカプセル化することである。

プロトコル変換は分割プロキシによって達成される。ローカル・プロキシはホストで始動され、そこではユーザは標準Webブラウザも起動している。Web

ブラウザはローカル・プロキシと通信するように、ユーザまたはローカル・プロキシによって構成されている。後者の構成オプションの方が好ましいのは、このオプションを選ぶと、かなり込み入ったプロキシ構成上の問題がユーザから隠されるためである。しかし、プロキシはどのブラウザが使用されているかを知っていなければならない。

ローカル・プロキシとWebブラウザが起動され、正しく構成されると、ブラウザはすべてのWWW要求をローカル・プロキシに渡していく。ローカル・プロキシはブラウザのWWW要求を受け取ると、その要求を使用中のネットワークに見合った低バンド幅最適化プロトコルに変換する(例えば、UDP/IPをベースとするAirBoss(商標) ワイヤレス・トранスポート・プロトコル)。

リモート・プロキシは変換されたスクリプト形式をローカル・プロキシから受信し、ブラウザによって行われたオリジナル要求のためにオペレーションを遂行する能力を備えている。変換された要求からデータがリモート・プロキシで受信されると、そのデータはオリジナル・スクリプトに基づいて暗号化され、圧縮され、フィルタリングされ、および／または最適化プロトコルにカプセル化され、ローカル・プロキシに返送される(これらのサービスは下述するメソッド2と3の個所で詳しく説明されている)。ローカル・プロキシはカプセル化された応答を受信し、それをアンパッケージし、最終的応答をブラウザに戻す。

次に図3を参照して、WWWデータの要求例について説明する。Webブラウザ54は、TCP/IPを構成しているアドバンストOSIプロトコル層またはアプリケーション層プロトコル70に置かれている要求を出力する。この要求はローカル・プロキシ56に送られ、そこで要求はAirBoss(商標) ワイヤレス・トランスポート・プロトコルなどのように、UDP/IPをベースとする低バンド幅最適化プロトコル72に変換される。次に、カプセル化された要求(以下、「カプセル化要求」という)はネットワーク・アクセス・デバイス58(例えば、モデム)を経由して低バンド幅ネットワークに渡される。

図4に示すように、要求は低バンド幅ネットワークを通り抜けて、総称(general)サービス・ノード74に到達する。その後、カプセル化要求はリモート・

プロキシ 6 に渡され、そこでカプセル化要求は低バンド幅最適化プロトコル（例えば、AirBoss（商標）トランSPORT・プロトコル）から、Web ブラウザが作成した元のアプリケーション層プロトコルに変換され、ブラウザの要求がインターネットに渡される。

リモート・プロキシとローカル・プロキシとの間の通信に関しては、マルチスレッディング(multi-threading)が重要である。ここでマルチスレッディングとは、アプリケーションが複数のオペレーションを同時に実行しているように見えるようにするプログラミング／オペレーティング・システム・パラダイムのことである。本発明の開発過程で分かったことは、分割プロキシに要求／応答のペアをマルチスレッディングできる能力をもたせることである。大部分のWWW ブラウザはマルチスレッドされたクライアント要求／応答をサポートしているので、分割プロキシにも同じことができる能力をもたせて、WWW アクセス体制にシームレスに統合化できるようにする必要がある。

本発明の分割プロキシでマルチスレッディングを実現するためには、要求をカプセル化している内部スクリプトを、ブラウザを宛先とする応答スクリプトと突き合わせるためのトランザクション・システムがローカル・プロキシとリモート・プロキシの間に必要である。これらのプロキシの間にどのようなトランザクション・システムが実現されるかは重要ではなく、また、トランザクション・システムが本発明の開示内容に基づいてどのように構築されるかは、この分野の通常の

知識を有するものには自明のことである。メソッド・セット 1 と 2 に説明されているプロトコルとトランザクション・メカニズムは'336出願に記載されているパーソナル・コミュニケーションズ・インターネット(Personal Communications Internet-PCI) 作業システムをベースにしている。

トランザクション・システムが高精度化すれば、本発明のシステムと方法はそれだけ効率化するので、エンドユーザが低バンド幅ネットワーク上でWWWをブラウズすることが可能になる。以下に説明する本発明のメソッドは上記事実に基づいている。

マルチスレッドされた要求／応答ペアをサポートする利点は、複数のブラウザを単一のローカル・プロキシによってホスト上でサポートできることである。

メソッド・セット2

開発されたWWWと既存プロトコルはユーザのデータ伝送要求に応えるように相互の上に階層化されていたので、Webブラウザは既存プロトコルを利用するようになっていた。現存WWWアクセス・ソフトウェアでは、データ・セキュリティとコンパクト化の要求は大部分が無視されていた。その結果、TCP/IPを使用するWebブラウザは伝送すべきデータを暗号化し、圧縮し、あるいはフィルタリングする機能を備えていない。

WWWの主要コンソーシアムであるW3Cは、WWW上のデータ伝送の安全保護に関する標準を検討している。しかし、このようなWebワイドの標準には、この標準がいったん公表されると、ハッカがそのプロトコル仕様の中に押し入っていき、安全保護措置を打ち破る方法を見つけるという問題がある。

従って、本発明の目的は、WWWがオープンであるとの性格をすべてまだ利用している自社所有体制において、プロキシ・ソフトウェアに圧縮、暗号化、およびフィルタリングの各ツールを組み入れたことである。従って、リモート・プロキシとローカル・プロキシの間のトランザクション・システムは圧縮および暗号化アルゴリズムを備えているので、自社カストマが使用するようにサービス・プロバイダによって設計された自社所有システムにすることができる。

フィルタリング・ツールは分割プロキシによって実現することも可能である。本発明でフィルタリングというときは、低バンド幅ネットワーク上のグローバル制御のことである。例えば、ブラウザが情報要求を出すとき、どれだけの情報が検索されるかが分かっていないのが一般である。本発明の原理によれば、ローカル・プロキシがフィルタリング構成命令をユーザから受け取ると、その命令はリモート・プロシキに送られて、そこで実行される。この場合、リモート・プロキシは、ユーザのデータ要求に対する応答を調べたり、例えば、不当に大きなデータ・オブジェクトがユーザのシステムを圧倒するのを防止するといった、機能を実行することができる。

一般的に、暗号化および圧縮アルゴリズムは、新しいWebブラウザに置いておくのではなく、ローカル・プロキシとリモート・プロキシの間に置いた方が好都合である。上述したように、この種のアルゴリズムは自社所有体制で保護することができる。この分野の通常の知識を有する者ならば、暗号化および圧縮アルゴリズムは独自のアルゴリズム・セットを望んでいるサービス・プロバイダのために周知の原理に基づいて容易に設計することが可能である。

これに対して、この種のアルゴリズムに関するオープンで、広く知られた標準は、例えば、W3Cで検討されているものと同じように、批判されているにもかかわらず、例えば、相互運用性(interoperability)といった長所をもっている。相互運用性とは、プロキシの異なる作成者が一緒に機能するリモート・プロキシとローカル・プロキシを作成できるようにすることである。また、異種コンピュータ・プラットフォームのメーカーが自社プラットフォームを他社プラットフォームとプリッジさせることも可能にする。

圧縮、暗号化およびフィルタリングを実現するスクリプトは、それが自社所有であるか、オープンであるかに関係なく、少なくとも次のことを実行するフィールドを含んでいる必要がある。

A. 暗号化のサポート。例えば、電子データの通貨取引を安全保護するMD5暗号化(cipher)アルゴリズム。

B. 複数のタイプの圧縮のサポート(どのタイプの圧縮を選択するかはスクリプトに含まれるデータのタイプに基づいて行う必要がある)。例えば、テキスト・データにはLZW圧縮アルゴリズムが使用できる。

C. 少なくとも負フィルタまたは正フィルタのサポート。例えば、次のフィルタリング・アルゴリズムの1つまたは2つ以上が使用できる。

負フィルタ - 応答スクリプトはどのバイナリ・データも含んでいてはならない。また、応答スクリプトはこのサイズより大であってはならない。

正フィルタ - 応答はそこに「ワイヤレス」が入っているすべてのテキスト行を含んでいかなければならない。

リモート・プロキシとローカル・プロキシの間の通路上のいずれかの箇所に、

なんらかの障害が起ったとき、特にワイヤレス環境では、ローカル・プロキシとリモート・プロキシの間のトランザクション・システムはその障害に見合う応答ができなければならない。例えば、スクリプトをワイヤレス・ネットワークに渡すことができないとか、あるいはスクリプトがリモート・プロキシに到達できないとか、あるいはリモート・プロキシがインターネットへのアクセス権を得ることができないときは、トランザクション・システムはそれに見合う応答ができなければならない。

メソッド・セット3

最後の問題は、WWWアクセス・ソフトウェアであるWebブラウザが最初からクライアントとして働くように設計されていたために発生するものである。クライアント・ソフトウェアはそれ自体、ネットワークからの非同期または非送信請求更新を受信できないのが一般的である。これは、サービス・プロバイダが加入者にアクセス・ソフトウェアを提供した後で、そのソフトウェアの構成をユーザのためにリモートで（ネットワーク内から）管理したい場合に問題となる。本発明の特徴によれば、大規模のサービス・プロバイダはカストマの要求に合わせて拡張可能なWWWアクセスを提供することができる。

上述したように、現在使用されているWebブラウザはこのような更新を受信し、それを実現する設計になっていない。その代わりに、サービス・プロバイダは新しい更新済みソフトウェアを配布している。ユーザが大規模で稼働している場合には、更新を実現するためには、ソフトウェアを再インストールし、ソフトウェアを再構成し、その障害診断を行うために派遣されたサービス・エンジニアが必要になる場合さえある。別の方法として、カストマはカストマ・サポート・ラインに電話し、更新のインストールをサポートする口頭の指示を待たなければ

ならない場合もある。

本発明の原理によれば、もっと単純で、もっと効率的な解決方法は分割プロキシ・インターフェースを使用してサービス・プロバイダから提供される。サービス・プロバイダのシステム用に設計された暗号化およびセキュリティ・プロトコルを使用すると、サービス・プロバイダはユーザ自身のシステムに置かれているユ

ーザのWWWアクセス・ソフトウェアにアクセスし、そのソフトウェアを即時にインストールし、構成し、あるいは更新することができる。このメソッドには、サービス・プロバイダによってとられたアクションをユーザに知らせるメッセージを組み入れることもできる。

本発明の解決方法(solution)は、ソフトウェア更新、構成の変更、または新規サービスの広告といった事柄に合わせてエンドユーザのホスト・システムを変更することを目的としたスクリプトを非同期／非送信請求で受信できるようにローカル・プロキシを構成することである。ローカル・プロキシはユーザのシステムのバックグラウンドで実行させて、Webブラウジング・ソフトウェアが実行中でない場合でも、上記のような通知を受信して、実現するようにすることが理想である。

ローカル・プロキシはブラウザの一部ではないため、これらの非同期ネットワーク・アップロードを受信するために常時実行させておく必要があるので、本発明はシステム・リソースの量を制限するために小サイズで、モジュール構造の設計になっている。この特徴は、インストールされている他のソフトウェアとの望ましくないやりとりから保護する(つまり、メモリ割り振り、IPポート割り当てなど)。

好適な実施(インプリメンテーション)

以下では、図5を参照して本発明のフロー・ダイヤグラムについて説明する。図5に示したフロー・ダイヤグラムは、本発明の主要コンポーネントに対応する一連のエンティティが上段にリストされている。つまり、Webブラウザ54、ローカル・プロキシ56、リモート・プロキシ66、およびWWWの外部Webサーバ68である。このフロー・ダイヤグラムはスタートアップ・プロセス期間、一般ブラウザ使用プロセス期間、およびサービス更新プロセス期間のそれぞれに

おいて、これらのコンポーネントがどのように作用し合うかを示している。

Webブラウザ54とローカル・プロキシ56は、同じホスト・コンピュータまたはユーザ端末52上に共存して実行される設計になっている。しかし、リモ

ート・プロキシ6 6と外部Webサーバは必ずしも共存させる必要はない。リモート・プロキシ6 6は外部Webサーバだけにアクセスして、通信できるようになつていなければならない。

図5の矢印はデータが一方のエンティティから他方のエンティティに通知または転送されることを示している。矢印のヘッドはアクションが指示される方向を示している。上から下へのラインはプロセス・ステップが実行されるときの時間ラインと順序を示している。

図5に示す最初のフローはスタートアップ・フローである。これは基本的に、システムがエンドユーザのホスト・コンピュータでどのようにアクチベートされるかを示している。ここでは、リモート・プロキシと外部Webサーバは、以下のフロー説明のいずれにおいても、すでに実行中であると想定している(これらのシステムは、エンドユーザ側から見たとき、どのやりとりもしないで、システム管理者が保守し、始動できるようになっている)。最初に行われるアクションはエンドユーザがローカル・プロキシを始動することである。これは、マルチスレッド・オペレーティング・システムのバックグラウンドで始動され、実行されるアプリケーションを起動することを意味するだけである。オペレーティング・システムは、例えば、Windows(商標)バージョン3.1オペレーティング・システムにすることができる。

ローカル・プロキシが始動された後、ローカル・プロキシは2つのことを行う責任がある。ブラウザ・タイプがユーザのホスト・コンピュータで指定されていれば、ローカル・プロキシはそのブラウザを構成して始動しなければならない。ブラウザには、その起動前に構成しておかなければならないものと、起動してから構成しなければならないものとがある。これはどのブラウザ・タイプが使用されるかによって決まる。ブラウザはプロキシ・サービスをサポートする従来のブラウザ・タイプならば、どのタイプであっても構わない。

どのブラウザ・タイプであるかが分かつていないときは、エンドユーザはそのブラウザを手作業で始動して、ローカル・プロキシ用に構成する必要がある。この場合、エンドユーザは使用しようとするWebブラウザに関する情報が十分に

分かっていて、プロキシ・サービス用にそのプラウザを手作業で構成できるようになっていなければならない。

図5に示す第2のフローは一般ブラウザ使用フローである。このフローはブラウザが始動され、構成された後の本発明のプロセス・ステップを示している。エンドユーザはまず標準Web要求を渡す。これは、基本的には、ユーザがハイパーアリンクでポイントし、クリックするか、あるいはダイアログ・ボックスを開き、一般に汎用リソース・ロケータ(universal resource locator-URL)と呼ばれているものに入ることを意味している。例えば、これはインターネット・コミュニティがWWW上のデータ・オブジェクトをどのように識別し、アクセスするかの方法である。

一般ブラウズ使用のフローの次のステップは、ブラウザから起動された照会がローカル・プロキシに渡されることである。ローカル・プロキシは照会スクリプトを作成し、データ・オブジェクトで使用される圧縮のタイプまたは利用できる圧縮のタイプを定義している設定値をそのスクリプトに入れる。ローカル・プロキシは、そのデータ・オブジェクトに適用されるフィルタと暗号化のタイプに関する設定値もスクリプトに入れる。これらの設定値はセキュリティを提供し、照会に対する応答として戻される情報をユーザが制御できるようにもする。

そのスクリプトが作成されると、これはリモート・プロキシに送付される。リモート・プロキシは照会スクリプトを解析し、ブラウザから最初に渡されたパッケージ化照会を抜き出す。リモート・プロキシは、次に、標準Webデータ・オブジェクト要求の中の照会を実行する。

外部Webサーバは照会を受信した後、その照会に関連する該当データ・オブジェクトを返却する。この時点では、他の特殊な強化機能は不要である。これはどの該当WWWプロトコルでも使用できるコンピュータ・ネットワーク上の従来のクライアント/サーバ要求にすぎないからである。例えば、ハイパーテキスト転送プロトコル、ファイル・トранSPORT・プロトコル、シンプル・メール・トランSPORT・プロトコル、またはポストオフィス・プロトコルが使用できる。

データ・オブジェクトがリモート・プロキシに戻されると、リモート・プロキシはオリジナル照会スクリプトの中で指定されていた圧縮、フィルタ、および暗号化を適用する。この中には、データ・オブジェクトをローカル・プロキシに渡すのに正しい形式に入れるためにデータ・オブジェクトに対して実行されるアクションが含まれる。圧縮、フィルタ、および暗号化は形式化されて応答スクリプトに入れられる。

アクションが完了し、ローカル・プロキシに渡されると、ローカル・プロキシは応答スクリプトを要求スクリプトと突き合わせる。応答スクリプトが要求スクリプトと突き合わされた後、該当ブラウザと、その情報をブラウザに送るべき場所を知ることになる。次に、ローカル・プロキシは応答スクリプト全体にわたって解析し、内部データ・オブジェクトを抜き出す。従って、ローカル・プロキシ側では、応答スクリプトについて2つのことが行われる必要がある。応答スクリプトは要求と突き合わされなければならず、ローカル・プロキシはデータ・オブジェクトを抜き出し、それをオペレーティング・システム内の該当場所に送ってブラウザがオブジェクトをそのビュアで表示できるようになっていなければならぬ。

図5に示す第3のフローはサービス更新またはサービス・スクリプト・フローである。これは、更新されたサービスを実現することに关心を持つネットワーク管理者がネットワーク内からリモートでエンドユーザのホスト・システムを構成できるような場合に行われる。リモート・プロキシはサービス・スクリプトを作成する。例えば、新しいHTMLホームページが送付され、エンドユーザのリモート・システム側に構成される場合には、HTMLファイルを配布(distribution)の中に書くようにローカル・プロキシに指示するサービス・スクリプトが作成されることになる。このサービス・スクリプトはHTMLページをデータ・オブジェクトとして含んでおり、このスクリプトが適切な形式で完成すると、ローカル・プロキシに送られる。

ローカル・プロキシはサービス・スクリプト全体を解析し、アクションおよびそのアクションに関連するデータ・オブジェクトを共に抜き出し、要求アクションを完了する責任がある。そこで、この例を終了するために、ローカル・プロキ

シはどのアクションが要求されたかを知るために全体を解析し(新しいHTMLホームページを書く)、データ・オブジェクト(新しいHTMLホームページ)を抜き出し、データ・オブジェクトをローカル・ファイル配布に書き込む。矢印は、該当する場合には、情報をブラウザに表示することがあることを示している。それが可能でないこともあるので、ローカル・プロキシは適切なアクションのダイアログ・ボックスまたは他のユーザ・インターフェース通知を表示する。非同期更新を受信できるブラウザにはその時点で通知することができ、ローカル・プロキシはそのアクションを開始し、適切なユーザ・インターフェース・コントロールがあれば、それをブラウザに送信してローカル・ホスト・システムで実行されたばかりのアクションをユーザに表示する。

本発明によって提供されるユーザとWWWとの間のインターフェースはプロトコル変換、圧縮、暗号化、フィルタリングおよび自動サービス更新の機能を備えているので、この非常に高価なリソースとのコネクションが大幅に向上される。圧縮に関しては、本発明のプロキシ・サービスをワイヤレス・ネットワーキング環境で要求するときのエンドユーザの直接費用が節減されることになる。大部分のワイヤレス・ネットワーク・プロバイダはパケット当たりの料金を提供し、大量(バルク)使用については均一料金(例えば、1MBデータまで一定料金)を提供している。直接費用節減はそのリンク上のデータが圧縮されているとき実現することができる。実験に基づく測定で明らかになったことは、標準HTMLデータはスクリプトのオーバヘッドを含めて、オリジナル・ペイロードの50-60%まで正規に圧縮できることである。このことは、カストマは同じ価格で2倍のWWWデータを検索できることを意味する。

本発明によれば、ネットワーク管理者はカストマのホスト構成を直接に管理することができるので、問題診断のために信頼度の低いテクニカル・サポート・ラインを無視でき、またソフトウェアの込み入った設定値をカストマに学ばせる必要がなくなる。また、新しいサービスの配備は本発明によって自動化される。

本発明で具現化されているテクノロジはISP、PDAとラップトップのメーカー、ワイヤレス・ネットワーク・プロバイダ、ワイヤレス・システム統合業者、およびISPになることを希望しているテレホニ・プロバイダが使用するのに最

も適している。このテクノロジを他のプロダクト・ラインと統合化すると、WWWと強い結び付きをもち、移動可能コンポーネントをもつプロジェクトを強化することも可能である。

以上の説明から理解されるように、本発明は上述し、添付図面に図示されている正確な構成またはプロセス・ステップに限定されるものではなく、本発明の範囲と精神を逸脱しない限り種々態様に改良および変更を行うことが可能である。また、本発明の範囲と精神は請求の範囲に記載されている事項によってのみ限定されるものである。

【図 1】

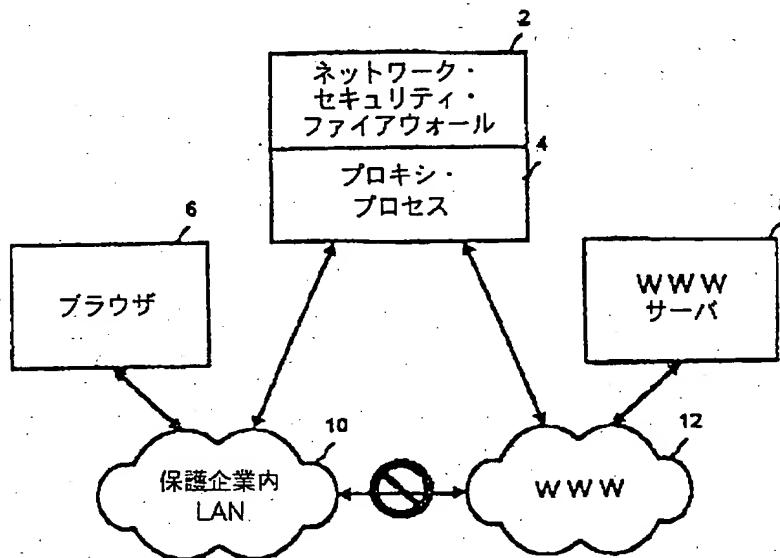


FIG. 1

(従来技術)

【図 2】

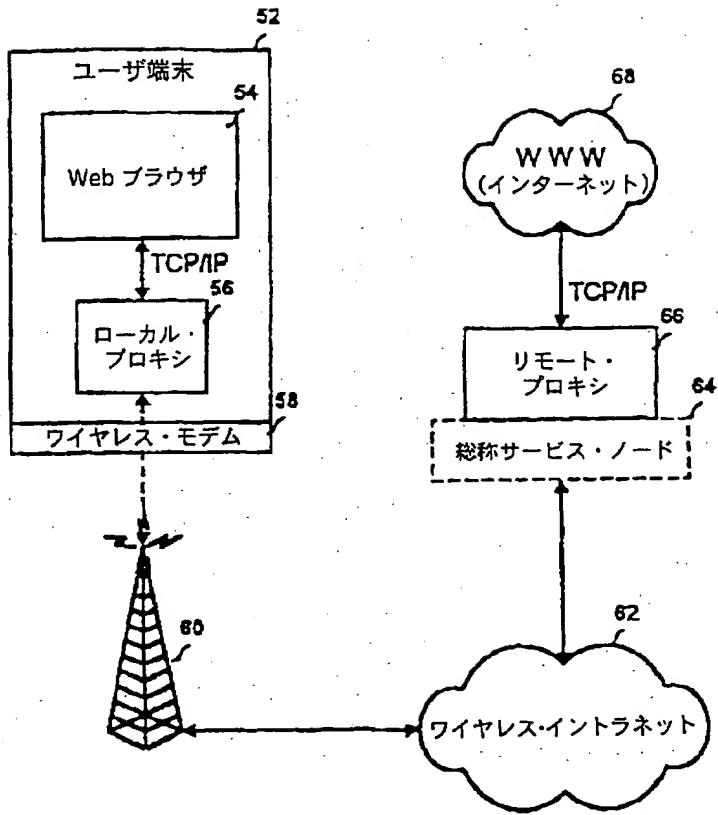


FIG. 2

【図3】

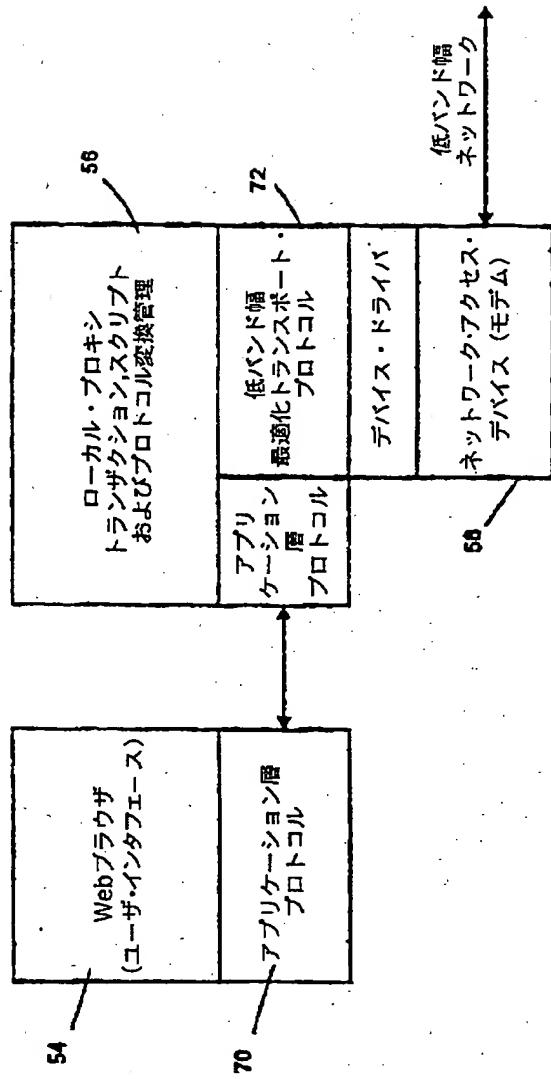


FIG. 3

【図 4】

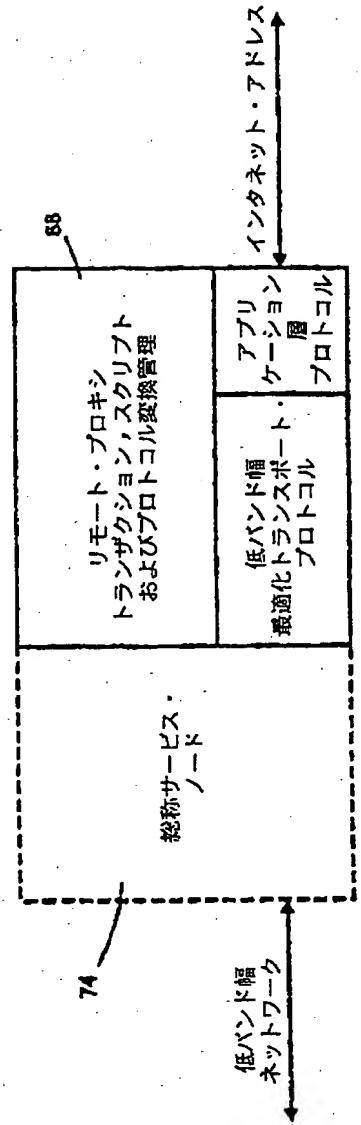
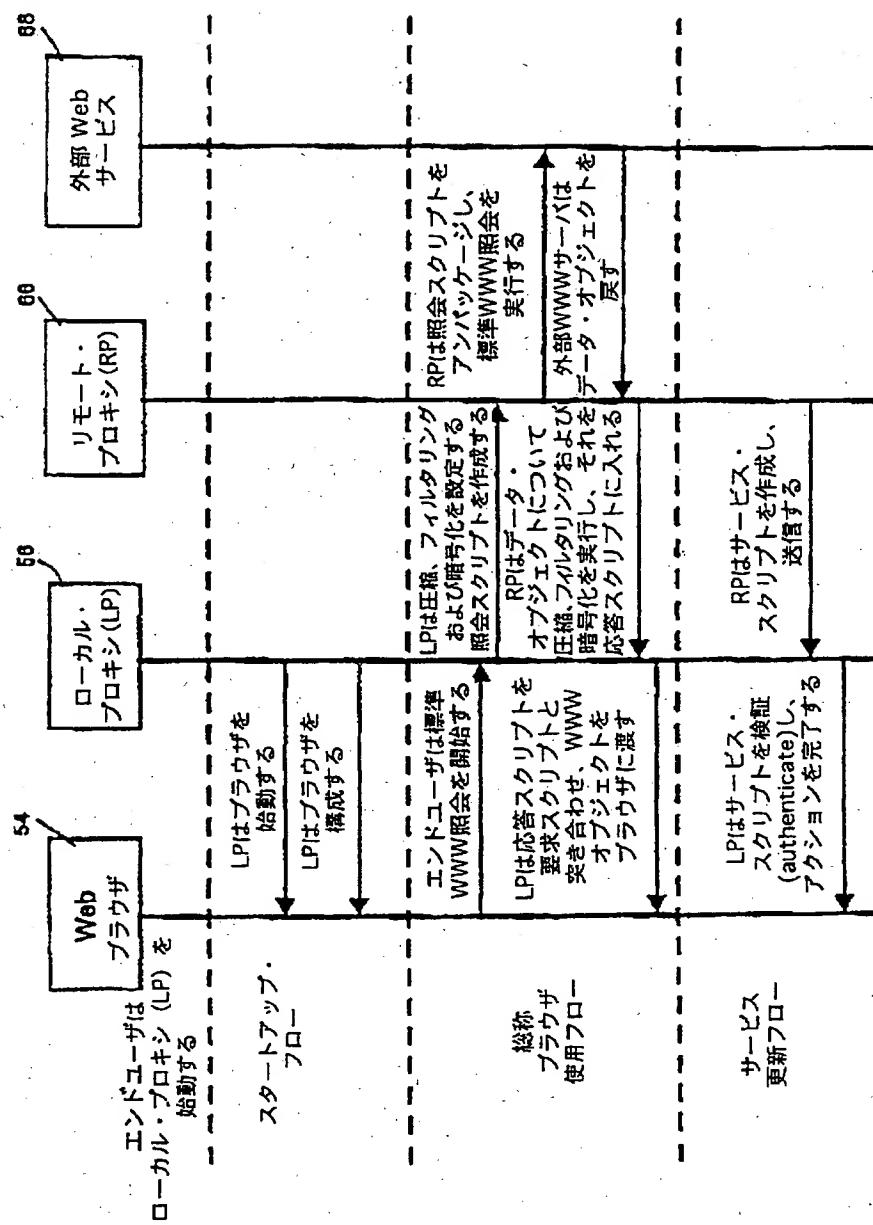


FIG. 4

[5]



5
G
E

【手続補正書】特許法第184条の8第1項

【提出日】1998年3月11日

【補正内容】

請求の範囲

1. 第1ロケーションに置かれておりクライアント・アプリケーションをもつホスト・コンピュータと、第2ロケーションに置かれているサーバ・アプリケーションとの間でコミュニケーション・パスを通して通信する方法であって、該方法は、

ローカル・プロキシを前記第1ロケーションに設置し、

前記コミュニケーション・パスを通して前記ローカル・プロキシと通信するリモート・プロキシを前記第2ロケーションに設置し、

前記クライアント・アプリケーションで照会を開始し、アプリケーション層プロトコルを使用して前記照会を前記ローカル・プロキシに送信し、

前記照会のアプリケーション層プロトコルをトランSPORT・プロトコルに変換し、

前記トランSPORT・プロトコルにおける前記照会を前記コミュニケーション・パスを通して前記ローカル・プロキシから前記リモート・プロキシに伝送し、前記伝送された照会のトランSPORT・プロトコルを、前記照会を前記サーバ・アプリケーションで実行するためのアプリケーション層プロトコルに変換することを含むことを特徴とする方法。

2. 請求項1に記載の方法において、前記コミュニケーション・パスは高レイテンシ・コミュニケーション・パスであることを特徴とする方法。

3. 請求項1に記載の方法において、前記コミュニケーション・パスはワイヤレス・ネットワークであることを特徴とする方法。

4. 請求項1に記載の方法において、さらに、

前記照会を前記サーバ・アプリケーションで実行し、データ・オブジェクトを前記リモート・プロキシに戻すステップを含むことを特徴とする方法。

5. 請求項4に記載の方法において、さらに、

前記データ・オブジェクトをトランSPORT・プロトコルに変換し、
前記データ・オブジェクトを前記トランSPORT・プロトコルに入れて、
コミュニケーション・パスを通して前記リモート・プロキシから前記ローカル・プ
ロキシに伝送し、

伝送されたデータ・オブジェクトの前記トランSPORT・プロトコルを前記
ローカル・プロキシでアプリケーション層プロトコルに変換し、

前記データ・オブジェクトを前記アプリケーション層プロトコルを使用して
前記クライアント・アプリケーションに伝達するステップを含むことを特徴とす
る方法。

6. 請求項1に記載の方法において、さらにスタートアップ・オペレーションを含み、該スタートアップ・オペレーションは、

前記ホスト・コンピュータで前記ローカル・プロキシを始動し、
前記ローカル・プロキシを使用して前記クライアント・アプリケーションを
構成し、始動するステップを含むことを特徴とする方法。

7. 請求項1に記載の方法において、前記照会の前記アプリケーション層プロトコルを変換する前記ステップは、さらに、

圧縮、フィルタ、および暗号化に関する設定をもつ照会スクリプトを作成し
前記照会スクリプトをカプセル化して、前記コミュニケーション・パスを通して前記ローカル・プロキシから前記リモート・プロキシに伝送するステップを含むことを特徴とする方法。

8. 請求項7に記載の方法において、前記データ・オブジェクトの前記アプリケーション層プロトコルを変換する前記ステップは、さらに、

前記照会スクリプトに含まれる前記設定に従って前記データ・オブジェクト
を圧縮し、フィルタリングし、暗号化し、
前記データ・オブジェクトを応答スクリプトに入れて、前記コミュニケーション・パスを通して前記リモート・プロキシから前記ローカル・プロキシに伝送するステップを含むことを特徴とする方法。

9. 請求項8に記載の方法において、さらに、

前記応答スクリプトを前記ローカル・スクリプトで受信したとき前記応答スクリプトを前記照会スクリプトと突き合わせ、
前記応答スクリプトを前記クライアント・アプリケーションに送付し、
前記データ・オブジェクトを前記応答スクリプトからアンパッケージし、
前記データ・オブジェクトを前記第1ロケーションで表示するステップを含むことを特徴とする方法。

10. 請求項1に記載の方法において、さらに、

サービス・スクリプトを前記リモート・プロキシで作成し、
前記サービス・スクリプトを前記リモート・プロキシから前記ローカル・プロキシに伝送し、
前記サービス・スクリプトを解析し、要求アクションとデータ・オブジェクトを前記サービス・スクリプトから抜き出し、
サービス・アクションを前記ローカル・プロキシで実行するステップを含むことを特徴とする方法。

11. 第1ロケーションに置かれておりクライアント・アプリケーションをもつホスト・コンピュータと、第2ロケーションに置かれているサーバ・アプリケーションと間で、コミュニケーション・パスを通して通信するシステムであって、該システムは、

第1ロケーションに置かれているローカル・プロキシと、
第2ロケーションに置かれており前記コミュニケーション・パスを通して前記ローカル・プロキシと通信するリモート・プロキシと、

前記クライアント・アプリケーションで照会を開始し、アプリケーション層プロトコルを使用して前記照会を前記ローカル・プロキシに送信する手段と、
前記照会のアプリケーション層プロトコルをトランスポート・プロトコルに変換する手段と、

前記照会を前記トランスポート・プロトコルに入れて、前記コミュニケーション・パスを通して前記ローカル・プロキシから前記リモート・プロキシに伝送

する手段と、

前記トランSPORT・プロトコルを、前記サーバ・アプリケーションで前記照会を実行するためのアプリケーション層プロトコルに変換する手段とを備えていることを特徴とするシステム。

12. 請求項1 1に記載のシステムにおいて、前記照会を実行する手段と、データ・オブジェクトを前記リモート・プロキシに戻す手段とをさらに備えていることを特徴とするシステム。

13. 請求項1 2に記載のシステムにおいて、さらに、

前記データ・オブジェクトをトランSPORT・プロトコルに変換する手段と

前記データ・オブジェクトを前記コミュニケーション・パスを通して前記リモート・プロキシから前記ローカル・プロキシに伝送する手段と、

前記データ・オブジェクトのトランSPORT・プロトコルを前記ローカル・プロキシでアプリケーション層プロトコルに変換する手段と、

前記アプリケーション層プロトコルを使用して前記データ・オブジェクトを前記クライアント・アプリケーションに伝達する手段とを備えていることを特徴とするシステム。

14. 請求項1 1に記載のシステムにおいて、さらに、

前記ローカル・プロキシを前記クライアント・アプリケーションで始動する手段と、

前記ローカル・プロキシを使用して前記クライアント・アプリケーションを構成し、始動する手段とを備えていることを特徴とするシステム。

15. 請求項1 1に記載のシステムにおいて、前記照会の前記アプリケーション層プロコトルを変換する前記手段は、さらに、

圧縮、フィルタ、および暗号化に関する設定をもつ照会スクリプトを作成する手段と、

前記照会スクリプトをカプセル化し、前記コミュニケーション・パスを通し

て前記ローカル・プロキシから前記リモート・プロキシに伝送する手段と
を含んでいることを特徴とするシステム。

16. 請求項 15 に記載のシステムにおいて、前記データ・オブジェクトの前
記アプリケーション層プロトコルを変換する前記手段は、さらに、
前記照会スクリプトに含まれる設定に従って前記データ・オブジェクトを圧
縮し、フィルタリングし、暗号化する手段と、

前記データ・オブジェクトを応答スクリプトに入れて、前記コミュニケーション・パスを通して前記リモート・プロキシから前記ローカル・プロキシに伝送
する手段と

を含んでいることを特徴とするシステム。

17. 請求項 16 に記載のシステムにおいて、さらに、
前記応答スクリプトを前記ローカル・プロキシで受信したとき前記応答スク
リプトを前記照会スクリプトと突き合わせる手段と、
前記応答スクリプトを前記クライアント・アプリケーションに送付する手段
と、

前記データ・オブジェクトを前記応答スクリプトからアンパッケージする手
段と、

前記データ・オブジェクトを前記第 1 ロケーションで表示する手段と
を備えていることを特徴とするシステム。

18. 請求項 11 に記載のシステムにおいて、さらに、
サービス・スクリプトを前記リモート・プロキシで作成する手段と、
前記サービス・スクリプトを前記リモート・プロキシから前記ローカル・プロキシに伝送する手段と、
前記サービス・スクリプトを解析し、要求アクションとデータ・オブジェクトを前記サービス・スクリプトから抜き出す手段と
を備えていることを特徴とするシステム。

19. 請求項 11 に記載のシステムにおいて、前記コミュニケーション・パス
は高レイテンシ・コミュニケーション・パスであることを特徴とするシステム。

20. 請求項19に記載のシステムにおいて、前記コミュニケーション・パスはワイヤレス・ネットワークを含むことを特徴とするシステム。

21. リモート・サーバと通信するシステムであって、該システムは、ユーザ・インターフェースのためのクライアント・アプリケーションをもつホスト・コンピュータと、

アプリケーション層プロトコルを使用して前記クライアント・アプリケーションと通信するローカル・プロキシであって、該ローカル・プロキシ手段は前記アプリケーション層プロコトルをトランスポート層プロトコルに変換する手段をもつものと、

トランスポート・プロトコルを使用して前記ローカル・プロキシと通信するリモート・プロキシであって、該リモート・プロキシは前記トранspoート・プロトコルを前記アプリケーション層プロトコルに変換する手段を含み、さらに、該リモート・プロキシは前記アプリケーション層プロトコルを使用して前記リモート・サーバと通信する手段を含むものとを備えていることを特徴とするシステム。

22. 請求項21に記載のシステムにおいて、前記ローカル・プロキシと前記リモート・プロキシは高レイテンシ・コミュニケーション・パスを通して通信することを特徴とするシステム。

23. 請求項21に記載のシステムにおいて、前記ローカル・プロキシと前記リモート・プロキシはワイヤレス・ネットワークを通して通信することを特徴とするシステム。

24. 請求項21に記載のシステムにおいて、前記プロキシはデータ伝送を暗号化するための少なくとも1つの暗号化アルゴリズムを備えていることを特徴とするシステム。

25. 請求項1に記載の方法において、前記プロキシにデータ伝送を暗号化するための少なくとも1つの暗号化アルゴリズムを装備することを、さらに含むことを特徴とする方法。

26. 請求項21に記載のシステムにおいて、前記リモート・プロキシは前記

ホスト・コンピュータへのデータ伝送をフィルタリングすることを特徴とするシステム。

27. 請求項1に記載の方法において、前記サーバ・アプリケーションから前記ホスト・コンピュータへのデータ伝送を前記リモート・プロキシでフィルタリングすることを、さらに含むことを特徴とする方法。

28. 請求項21に記載のシステムにおいて、前記プロキシは前記サーバ・アプリケーションと前記ホスト・コンピュータとの間のデータ伝送を圧縮することを特徴とするシステム。

29. 請求項1に記載の方法において、前記サーバ・アプリケーションと前記ホスト・コンピュータとの間のデータ伝送を前記プロキシで圧縮するステップをさらに含むことを特徴とする方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US96/03909

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00

US CL :380/49

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbol)

U.S. : 380/49

370/60, 82, 90

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A, 4,438,511 (BARAN) 20 MARCH 1984, See Fig. 1	1-32
Y	US,A, 4,893,302 (HEMMANDY ET AL) 09 JANUARY 1990 See Figs. 1, 4 & 9.	1-32
Y	US,A, 5,021,949 (MORTEN ET AL) 04 JUNE 1991 See Figs. 1, 2, 8, 22, 26, 30, 31, 32 and Col. 6, lines 60-65.	
Y	US,A, 5,220,501 (LAWLOR ET AL) 15 JUNE 1993 See fig. 1.	1-32
Y	US,A, 5,416,842 (AZIZ) 16 MAY 1995, See Figs. 2-11.	1-32
Y	US,A, 5,448,561 (KAISER ET AL) 05 SEPTEMBER 1995 See Fig. 1.	1-32

Further documents are listed in the continuation of Box C. See patent family annex.

- | | |
|--|--|
| * Special categories of cited documents: | |
| "A" | document defining the general state of the art which is not considered to be of particular relevance |
| "B" | earlier document published on or after the international filing date |
| "C" | document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reasons (as specified) |
| "D" | document referring to an oral disclosure, use, exhibition or other means |
| "E" | document published prior to the international filing date but later than the priority date claimed |
| "F" | later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| "G" | document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| "H" | document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| "I" | document member of the same patent family |

Date of the actual completion of the international search Date of mailing of the international search report
26 AUGUST 1996 04 OCT 1996

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
Salvatore Cangialosi
SALVATORE CANGIALOSI
Telephone No. (703) 305-1837

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03909

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.: because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-5, 8-22, 29-31 drawn to a remote proxy system and method.
Claims 6-7, 23-28 drawn to an encryption and method and apparatus.
Claim 32 drawn to a data compression method.

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
 No protest accompanied the payment of additional search fees.

フロントページの続き

- (72)発明者 ブリッツァー, リサ, ピー。
 アメリカ合衆国 07726 ニュージャージ
 一州 マナラパン グラマーシー レーン
 10
- (72)発明者 ブロックマン, ジェームズ, ジョーゼフ
 アメリカ合衆国 08535 ニュージャージ
 一州 ベリネヴィル ランニング ブルック
 ク ドライブ 15
- (72)発明者 クルツ, ウィリアム
 アメリカ合衆国 07724 ニュージャージ
 一州 イートンタウン ヴィオラント コ
 ート 9
- (72)発明者 ハキム, ドワイト, オマール
 アメリカ合衆国 07747 ニュージャージ
 一州 マタワン ティナ プレイス 20
- (72)発明者 ホーヴェイ, リチャード, レイド
 アメリカ合衆国 08876 ニュージャージ
 一州 サマーヴィル ノース ブリッジ
 ストリート 168
- (72)発明者 クラマー, マイケル
 アメリカ合衆国 10471 ニューヨーク州
 ブロンクス フィールドストン ロード
 6136
- (72)発明者 ペトル, ドーン, ダイアン
 アメリカ合衆国 08812 ニュージャージ
 一州 グリーン ブローク ヘリテイジ
 ドライブ 18
- (72)発明者 ラマロッソン, ジョセファ
 アメリカ合衆国 07728 ニュージャージ
 一州 フリーホールド テランス テラス
 23
- (72)発明者 ラミレス, ジェラルド
 アメリカ合衆国 08807 ニュージャージ
 一州 ブリッジウォーター サニー スロ
 ープ ロード 3505
- (72)発明者 ワン, ヤンーウェイ
 アメリカ合衆国 07731 ニュージャージ
 一州 ハウエル ケンブリッジ ドライブ
 10
- (72)発明者 ホワイト, ロバート, ジー。
 アメリカ合衆国 07960 ニュージャージ
 一州 モーリスタウン ノウルウッド ド
 ライブ 20